

Szczegółowa specyfikacja techniczna (SST)

1. Przedmiot zamówienia:

- 1) Przedmiotem zamówienia jest **dostawa urządzeń do filtrowania ruchu sieciowego (sieć OT) wraz z centralnym systemem zarządzania (konsola zarządzająca) i subskrypcjami wraz z usługą wsparcia technicznego.**
- 2) W ramach zamówienia Zamawiający wymaga dostarczenia:
 - a) **TXOneTXIQHWM130001 [New] EdgeIPS-103** tj. urządzenie do filtrowania ruchu sieciowego (sieć OT) wraz z systemem ochrony IPS - **10** sztuk;
 - b) **TXOne TXIQLE1X1031 [New] EdgeIPS-103 SW License** na okres **12 miesięcy** (od dnia podpisania *Protokołu zdawczo-odbiorczego*) – tj. subskrypcja umożliwiająca korzystanie z zaawansowanych funkcji bezpieczeństwa (Deep Packet Inspection dla OT, automatyczne aktualizacje sygnatur, integracja z SIEM/SOC (Security Information and Event Management, Security Operations Center) na sprzęcie EdgeIPS-103, obejmująca również aktualizację bazy sygnatur – **10** sztuk;
 - c) **TXOne [New] EdgeOne** tj. konsola zarządzająca systemu IPS (1 szt.) wraz z **TXOKMVE2X0001 Virtual Appliance** tj. subskrypcja do zarządzania urządzeniami na okres **12 miesięcy** (od dnia podpisania *Protokołu zdawczo-odbiorczego*) – **10** sztuk;
 - d) **Wparcie techniczne** – zgodne z pkt. 3 ppkt 3 przedmiotowej SST.
- 3) Miejsce dostawy urządzeń: OPEC Sp. z o.o. ul. Opata Hackiego 14, 81-213 Gdynia
- 4) Przedmiot umowy rozliczany będzie na podstawie *Protokołu zdawczo-odbiorczego* podpisanego przez Zamawiającego bez uwag.

2. Szczegółowy opis wymagań dotyczących przedmiotu zamówienia:

- 2.1. **TXOneTXIQHWM130001 [New] EdgeIPS-103** tj. urządzenie do filtrowania ruchu sieciowego (sieć OT) oraz **TXOne TXIQLE1X1031 [New] EdgeIPS-103 SW License** tj. subskrypcja:
 - 1) **Wymagane ogólne funkcje urządzenia oraz subskrypcji:**

urządzenie przemysłowe, sprzętowy IPS (sonda IPS) z funkcją DPI dla protokołów przemysłowych wraz z ochroną przed cyberatakami działający na zasadzie reguł korelacyjnych znanych podatności z bazą sygnatur posiadającą opcję aktualizacji w okresie 12 miesięcy od dnia podpisania *Protokołu zdawczo-odbiorczego*. Urządzenie wyposażone w jedną parę portów monitorujących oraz osobny interfejs zarządzający (OOBM). Jako parę portów Zamawiający rozumie dwa interfejsy służące do przepuszczenia przez nie transmisji celem jej analizy w czasie rzeczywistym.
 - 2) **Wymagane funkcje urządzenia:**
 - a) hardware based IPS – niezależny od urządzeń końcowych hardware, nie dopuszcza się rozwiązań typu host based (instalowany na end-poincie);
 - b) urządzenie musi być wykonane w technologii rugged tj. bezwentylatorowe i pracować w zakresie temperatury pracy tj. -40-70 st. C;
 - c) dedykowany port zarządzający (OOBM);
 - d) urządzenie transparentne pod kątem adresacji IP dla urządzeń/segmentów sieci podlegających ochronie;

- e) możliwość wpięcia urządzenia w linię z kluczowym assetem lub segmentem sieci - analiza i praca na rzeczywistym ruchu sieciowym, a nie na jego kopii;
- f) możliwość przekierowania ruchu ze SPAN portu na urządzenie - analiza i praca na kopii ruchu sieciowego;
- g) możliwość pracy w dwóch trybach:
 - IDS: (tryb monitorowania): wszelkie naruszenia polityk bezpieczeństwa są wyłącznie rejestrowane (na urządzeniu oraz w konsoli zarządzającej);
 - IPS (tryb ochrony): wszelkie naruszenia reguł bezpieczeństwa są blokowane i rejestrowane na urządzeniu oraz w konsoli zarządzającej;
- h) mechanizm fail safe dla pary portów (w przypadku portów miedzianych)
 - możliwość skonfigurowania bypassu portów LAN w trzech trybach:
 - niezwłoczne wznowienie ruchu sieciowego w przypadku awarii urządzenia;
 - całkowite zablokowanie ruchu sieciowego w przypadku awarii urządzenia;
 - przekazywanie ruchu pomiędzy portami bez skanowania;
- i) LFPT – w przypadku odpięcia urządzenia podłączonego do jednego z portów, port drugi automatycznie przechodzi w status DOWN;
- j) opóźnienia wprowadzane do sieci nie mogą być większe niż 520 us;
- k) Virtual Patching – ochrona przed znanymi podatnościami:
 - wirtualna aktualizacja urządzeń oparta o silnik sygnaturowy,
 - aktualizacje sygnatur nie mogą wymagać stałego dostępu do internetu - wymagana jest obsługa w środowisku on-premise;
- l) głęboka inspekcja pakietów dla protokołów OT:
 - możliwość wykorzystania sondy do tworzenia białej listy komend dla protokołów przemysłowych;
 - wymagana jest możliwość zautomatyzowanego utworzenia profilu DPI na podstawie analizy rzeczywistego ruchu sieciowego - reguła nie może być automatycznie przyjmowana, a wymaga się aby takie akcje były każdorazowo autoryzowane przez administratora;
 - wsparcie dla protokołów Modbus TCP, DNP3, IEC-103, S7COMM, PROFINET, FANUC:
 - dla protokołów Modbus oraz DNP3 wymaga się, aby profile DPI realizowały inspekcję głębszą aniżeli tylko rozpoznawanie portokołu:
 - dla protokołu DNP3 wymaga się, aby w ramach profilu DPI można było zdefiniować konkretny kod wiadomości np. 0x07 Immediate Freeze;
 - dla protokołu Modbus TCP wymaga się, by w ramach profilu DPI można było zdefiniować konkretne funkcje i rejestry np. 0x0F Write Multiple Coils;
- m) zautomatyzowane tworzenie reguł firewalla oraz profili DPI w trybie nauki na podstawie analizy ruchu rzeczywistego:
 - reguły nie mogą być automatycznie przyjmowane; każde przyjęcie reguły musi być autoryzowane przez administratora;
 - tryb nauki musi mieć możliwość uruchomienia na okres co najmniej do 7 dni kalendarzowych - tryb nauki nie może pracować w trybie ciągłym tj. winien być automatycznie wyłączony po określonym czasie;
 - tryb nauki musi mieć możliwość ponownego uruchomienia celem zaproponowania nowych reguł np. w przypadku modernizacji infrastruktury Zamawiającego;

- reguły proponowane po ponownym uruchomieniu trybu uczenia nie powinny powtarzać się względem już nauczonych;
- n) urządzenie musi być dostarczane wraz z konsolą zarządzającą z zapewnieniem obsługi wszystkich portów urządzenia.

2.2. **TXOne [New] EdgeOne** tj. konsola zarządzająca systemu IPS (centralny system zarządzania)

Wymagane funkcje:

- a) możliwość grupowego zarządzania sondami IPS z poziomu aplikacji centralnej;
- b) możliwość zdefiniowania globalnych reguł bezpieczeństwa przypisanych dla poszczególnej grupy urządzeń;
- c) możliwość agregowania logów z sond IPS w jednym miejscu:
 - przesyłanie logów na temat zdarzeń do oprogramowania SIEM z poziomu aplikacji centralnej;
- d) bieżąca aktualizacja bazy sygnatur w sondach, przez okres 12 miesięcy od dnia podpisania *Protokołu zdawczo-odbiorczego*;
- e) konsola musi mieć możliwość pracy bez konieczności podłączenia do internetu;
- f) udzielenie uprawnień lokalnym administratorom np. do zarządzania grupą urządzeń należącym do ich systemu, segmentu lub oddziału.

2.3. **TXOKMVE2X0001 Virtual Appliance** tj. subskrypcja do zarządzania urządzeniami na okres **12 miesięcy** (od dnia podpisania *Protokołu zdawczo-odbiorczego*):

- a) subskrypcja roczna producenta ze wsparciem producenta i prawem do aktualizacji;
- b) subskrypcja osobna dla każdego urządzenia.

3. Gwarancja oraz wsparcie:

- 1) Gwarancja sprzętowa tj. gwarancja producenta na urządzenia: **24 miesiące** od dnia podpisania *Protokołu zdawczo-odbiorczego*.
- 2) Wsparcie producenta w zakresie subskrypcji tj. licencja na aktualizacje sygnatur dla nośników (urządzeń) oraz konsoli zarządzającej: **12 miesięcy** od dnia podpisania *Protokołu zdawczo-odbiorczego*.
- 3) **Wsparcie techniczne** tj. Wykonawca będzie realizował usługę na rzecz Zamawiającego w zakresie wsparcia technicznego w utrzymaniu i rozwoju produktów: **12 miesięcy** od dnia podpisania *Protokołu zdawczo-odbiorczego*. Zakres usługi wsparcia technicznego:
 - a) Obsługa incydentów i zgłoszeń technicznych - wsparcie Zamawiającego w rozwiązywaniu problemów związanych z działaniem oprogramowania.
 - b) Utrzymanie i aktualizacje - wsparcie Zamawiającego i usługa konsultingowa w zakresie rozwoju konfiguracji, wdrażania poprawek producenta, aktualizacji oraz zapewnienie stabilnej pracy rozwiązania.
 - c) Rozwój i konfiguracja funkcjonalna - wsparcie Zamawiającego w dostosowaniu i rozbudowie systemu zgodnie z potrzebami Zamawiającego.
 - d) Wsparcie bezpieczeństwa i zgodności - rekomendacje konfiguracyjne, reagowanie na zgłoszenia kierowane od Zamawiającego do Wykonawcy, w tym reguł bezpieczeństwa.
 - e) Wsparcie techniczne winno być realizowane od poniedziałku do piątku w godzinach 7:00-15:00.